

4. Plaintiff Jane Doe 2 (“Doe 2”) is a U.S. citizen and is a resident of the Commonwealth of Virginia. She is an employee of an agency in the United States Executive Branch.

5. Similarly situated individuals include all employees of agencies in the United States Executive Branch who have been instructed to respond to either of two emails sent to their work email addresses from HR@opm.gov pursuant to an alleged “test” of a new “distribution and response list,” regardless of whether they responded to the alleged “test,” as well as all other employees of agencies in the United States Executive Branch whose information is stored in one or more systems affiliated with this “distribution and response list” but who have not yet received any “test” emails.

6. Defendant Office of Personnel Management (“OPM”) is an agency of the United States Executive Branch and is in control of the system(s) which are the subject of this action.

CLASS ACTION ALLEGATIONS

7. This action is brought by Plaintiffs on their own behalf and on behalf of the class of all others similarly situated under the provisions of Fed. R. Civ. P. 23(a) and (b)(1)-(2).

8. The class so represented by Plaintiffs in this action, and of which they are members, consists of anyone who received a request between 23-27 January 2025 to respond to HR@opm.gov to confirm that they received a response, as well as any U.S. Executive Branch employees whose information is stored in the system in question but who did not receive a “test” email.

9. The exact number of members of the class, as hereinabove identified and described, is not known, but it is reasonable to believe the class is so numerous that joinder of individual members is impractical.

10. The relief sought is common to the entire class, and there are common questions of law and fact that relate to and affect the rights of each member of the class. These common questions include and involve whether OPM can legally operate the system(s) in question without first publishing a Privacy Impact Assessment. Certain defenses raised by OPM would apply equally to all members of the class.

11. The claim of Plaintiffs against OPM are typical of the claims of the class in that the claims of all members of the class depend on a showing of the acts of OPM as giving rise to rights to the relief sought herein. There is no conflict as between Plaintiffs and other members of the class with respect to this action, or with respect to the claims for relief contained herein.

12. Plaintiffs are representative parties for the class and are able to and will fairly and adequately protect the interests of the class. Plaintiffs' undersigned counsel is experienced and capable in litigating the claims at issue and has represented claimants in other matters of this nature.

13. This action is properly maintained as a class action in that the prosecution of separate actions by individual members of the class would create a risk of adjudications with respect to individual members of the class which would as a practical matter be dispositive of the interests of others not party to the adjudications, or would substantially impair or impede their ability to protect their interests.

14. This action is properly maintained as a class action inasmuch as the questions of law and fact common to the members of the class predominate over any questions affecting only individual members, and a class action is superior to other available methods for the fair and efficient adjudication of the controversy.

BACKGROUND

Part I: The OPM Emails

15. On 23 January 2025, OPM published an official statement: “OPM is testing a new capability allowing it to send important communications to ALL civilian federal employees from a single email address. Testing of this messaging system functionality is expected as soon as this week.”

16. Beginning 23 January, some U.S. Executive Branch agencies began sending employees messages from senior officials advising that any emails received from HR@opm.gov should be considered legitimate. For example, on 23 January, the Acting Secretary of Homeland Security sent the following message to all Department of Homeland Security employees: “The Office of Personnel Management (OPM) is testing a new capability allowing it to send important communications to ALL Federal employees from a single email address, HR@opm.gov. If you ever receive communications from this address, it can be considered trusted.”

17. On 24 January, Plaintiffs received an email from HR@opm.gov stating: “This is a test of a new distribution and response list. Please reply ‘YES’ to this message.” The email included a hyperlink to the 23 January OPM announcement. Also on 24 January, Doe 1 was advised by senior agency attorneys to follow the instructions in the email and reply.

18. On 26 January, Plaintiffs received an email from HR@opm.gov stating:

This is the second test of a new email distribution and response list. The goal of these tests is to confirm that an email can be sent and replied to by all government employees.

Please reply “Yes” to this email, regardless of whether you replied to the first test email.

If you responded “Yes” to the first email: thank you. As a reminder, always check the From address to confirm that an email is from a legitimate government

account and be careful about clicking on links, even when the email originates from the government.

19. On 27 January, Doe 2 sent the reply “Yes” to HR@opm.gov in response to the 26 January OPM email.

20. As of this writing, Doe 1 has not responded to either email from HR@opm.gov.

Part II: The Unknown OPM Email Server

21. On 27 January, an unknown OPM employee posted a message to a “Union chat” which was later uploaded to <https://Reddit.com> (“Reddit Message”). This message provided much more detail about the origin and nature of the OPM “distribution and response list.”

22. According to the Reddit Message, posted by “an OPM employee for nearly a decade and a Federal Employee for almost 20 years,” incoming political appointees have “sent numerous requests to all the agencies to collect information on gov’t employees.” The Reddit Message further specifies, “Instructions say to send these lists to Amanda Scales. But Amanda is not actually an OPM employee, she works for Elon Musk.”

23. According to her LinkedIn page, Amanda Scales works for xAI, a private corporation, of which Elon Musk is the Chief Executive Officer.

24. According to the Reddit Message:

Our CIO, Melvin Brown, (also a non political career public servant) was pushed aside just one week into his tenure because he refused to setup email lists to send out direct communications to all career civil servants. Such communications are normally left up to each agency.

Instead, an on-prem (on-site) email server was setup. Someone literally walked into our building and plugged in an email server to our network to make it appear that emails were coming from OPM. It’s been the one sending those various “test” message you’ve all seen. We think they’re building a massive email list of all federal employees to generate mass RIF notices down the road.

25. Upon information and belief, this server and/or other systems linked to it are retaining information about every employee of the U.S. Executive Branch.

26. Upon information and belief, this server is not sending these or other emails securely due to the rapid deployment. Secure communications take time and coordination to plan and implement. Standard email is not encrypted, and it is common practice among hackers—including hackers affiliated with hostile foreign services—to begin attempting to access a new U.S. Government device as soon as they learn of its deployment.

CAUSE OF ACTION

(FAILURE TO CREATE PIAS)

27. Plaintiffs repeat and reallege the allegations contained in all paragraphs set forth above.

28. Under the E-Government Act of 2002, any agency “initiating a new collection of information that (I) will be collected, maintained, or disseminated using information technology; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual” is required to complete a Privacy Impact Assessment (“PIA”) before initiating such collection. *See* 44 U.S.C. § 3501 note.

29. The agency must “(i) conduct a privacy impact assessment; (ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and (iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.”

30. OPM is an agency subject to the E-Government Act because it is an “establishment in the executive branch of the Government.”

31. A PIA for a “new collection of information” must be “commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information.” The PIA must specifically address “(I) what information is to be collected; (II) why the information is being collected; (III) the intended use of the agency of the information; (IV) with whom the information will be shared; (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared; [and] (VI) how the information will be secured.”

32. OPM has not conducted a PIA for this unknown email server or any system which collects or maintains Personally Identifiable Information (“PII”) obtained from its use.

33. OPM has not ensured review of a PIA for any of these systems by any Chief Information Officer or equivalent official.

34. OPM has not published a PIA or made such an assessment available for public inspection for any of these systems.

35. OPM’s failure to take these steps constitutes agency action unlawfully withheld or unreasonably delayed in violation of 5 U.S.C. § 706(1).

36. Plaintiffs are being materially harmed by this inaction because they are being denied information about how these systems—which will be rich in PII about every employee of the U.S. Executive Branch—are being designed and used.

37. Plaintiffs stand to continue to be harmed by this ongoing inaction in the future beyond the informational injury, since they will face a reasonably foreseeable risk that their PII will be unlawfully obtained from these unknown systems, much as the data of millions of federal employees were unlawfully obtained from another OPM server in 2014.

38. Plaintiffs have a direct interest in ensuring that OPM conducts and publishes PIAs for these systems.

39. Plaintiffs are therefore entitled to relief in the form of an injunction prohibiting OPM from collecting or storing any information about employees of the U.S. Executive Branch in this unknown email server or any linked systems until it has conducted the necessary PIAs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Jane Does 1-2, and all other similarly situated individuals, pray that this Court:

(1) Declare and find that the Office of Personnel Management's failure to conduct and publish Privacy Impact Assessments for the unknown email server and any linked systems is a violation of the E-Government Act of 2002 by way of the APA, and that this violation was intentional and/or willful;

(2) Order OPM to promptly conduct PIAs about all such OPM systems prior to the collection of any PII using those systems;

(3) Order preliminary and permanent injunctive and/or declaratory relief as may be appropriate;

(4) Award reasonable costs and attorneys' fees as provided in 28 U.S.C. § 2412(d), or any other applicable law;

(5) Expedite this action in every way pursuant to 28 U.S.C. § 1657(a); and

(6) Grant such other relief as the Court may deem just and proper.

Date: January 27, 2025

Respectfully submitted,

/s/ Kelly B. McClanahan
Kelly B. McClanahan, Esq.
D.C. Bar #984704
National Security Counselors
1451 Rockville Pike
Suite 250
Rockville, MD 20852
501-301-4672
240-681-2189 fax
Kel@NationalSecurityLaw.org

Counsel for Plaintiffs